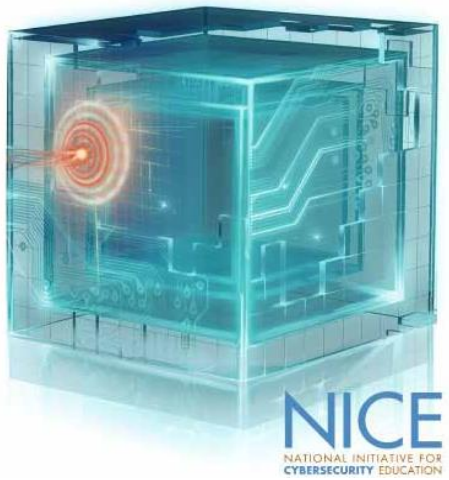
Homeland Security

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

USER GUIDE–

TRAINING VENDORS



Workforce Framework User Guide

Welcome to the User Guide!

The Workforce Framework helps **Training Vendors** create programs that are aligned to jobs.

The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework to categorize and define cybersecurity work.

When degrees, jobs, training and certifications are aligned to the Workforce Framework...
Colleges & Training Vendors can create programs that are aligned to jobs
Students will graduate with knowledge and skills that employers need
Employers can recruit from a larger pool of more qualified candidates
Employees will have a better defined career path and opportunities
Policy Makers can set standards to evolve the field

Workforce Framework User Guide

What's in this User Guide?

This guide was created to help you and your organization use the Workforce Framework. As you navigate through the guide, you will find:

- A Workforce Framework Overview.
- Benefits of implementing the Workforce Framework within your company/organization.
- Recommended steps for implementation.
- Useful tools and links that will help you promote and use the Workforce Framework.

The National Cybersecurity Workforce Framework

Led by the Department of Homeland Security (DHS), the National Initiative for Cybersecurity Education (NICE) raises public awareness, provides a foundation for the recruitment, training, and retention of cybersecurity professionals, and promotes cybersecurity education. The Workforce Framework (in support of the "Evolve the Field" goal) is a national resource providing employers, educators, trainers, and policy makers a common language for describing cybersecurity work.

The Workforce Framework contains cybersecurity Specialty Areas, knowledge, skills, and abilities (KSAs), tasks, and sample job titles. It has been updated to reflect the evolving cybersecurity field and incorporate diverse viewpoints across government, industry, and academia. Explore the Workforce Framework at the National Initiative for Cybersecurity Careers and Studies (NICCS™) website.

The Workforce Framework is:

A Blueprint

- Describes and categorizes cybersecurity work.
- Identifies sample job titles, tasks, and knowledge, skills, and abilities (KSAs).

A Tool

- Provides a foundation organizations can use to develop position descriptions, competency models, and training.

A Collaboration

- Incorporates inputs from industry, academia, and government.
- Addresses the nation's need to identify, qualify, and develop the cybersecurity workforce.

Using the Workforce Framework – Training Vendors

Having a common framework for describing cybersecurity work allows ***Training Vendors*** to use consistent language when designing and developing training courses and programs. Most importantly, it allows training vendors to align their courses and programs to a nationally recognized initiative.

Using the Workforce Framework, Training Vendors can:

- Use consistent language during the instructional systems design and development process.
- Offer courses tailored to the needs and requirements of cybersecurity professionals.
- Map courses to the Workforce Framework's Specialty Areas.
- List courses on the National Initiative for Cybersecurity Careers and Studies (NICCS) website.
- Attract cybersecurity professionals searching for training based on the Workforce Framework Specialty Areas.

Why is the Workforce Framework Important?

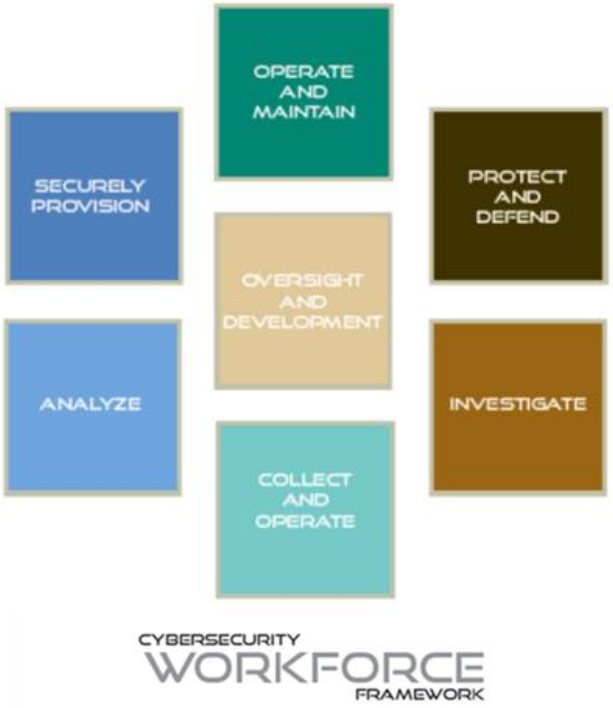
The Workforce Framework categorizes cybersecurity work and identifies cybersecurity Specialty Areas.

The Workforce Framework establishes:

- A common taxonomy and language which organizes cybersecurity work into seven Categories and more than 30 Specialty Areas.
- A baseline of tasks, Specialty Areas, and KSAs associated with cybersecurity professionals.

The Workforce Framework improves our Nation's ability to:

- Provide employers, educators, trainers, and policy makers a common language for describing cybersecurity work.
- Build and maintain the highly skilled and agile workforce needed to protect the nation.
- Coordinate and collectively address cybersecurity threats.



What are the Seven Categories?

The Workforce Framework's Categories organize Specialty Areas by grouping similar work.

Securely Provision	Specialty Areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty Areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty Areas responsible for identifying, analyzing, and mitigating threats to IT systems.
Investigate	Specialty Areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Collect and Operate	Specialty Areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty Area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Oversight and Development	Specialty Areas that provide critical support so others may conduct their cybersecurity work.

What are the Specialty Areas?

Specialty Areas describe a cybersecurity work area, or function. Each Specialty Area includes related Tasks, KSAs, and sample job titles.

Securely Provision
- Technology Research and Development
- Systems Requirements Planning
- Systems Security Architecture
- Software Assurance and Security Engineering
- Systems Development
- Test and Evaluation
- Information Assurance (IA) Compliance

Analyze
- Cyber Threat Analysis
- All Source Intelligence
- Targets
- Exploitation Analysis

Collect and Operate
- Operations Planning
- Cyber Operations
- Collection Operations

Protect and Defend
- Computer Network Defense (CND) Analysis
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense (CND) Infrastructure Support

Investigate
- Investigation
- Digital Forensics

Oversight and Development
- Strategic Planning and Policy Development
- Security Program Management (CISO)
- Information Systems Security Operations (ISSO)
- Education and Training
- Legal Advice and Advocacy

Operate and Maintain
- System Administration
- Network Services
- Customer Service and Technical Support
- Systems Security Analysis
- Data Administration
- Knowledge Management

National Initiative for Cybersecurity Careers and Studies (NICCS™)

For more information on the Workforce Framework, visit National Initiative for Cybersecurity Careers and Studies (NICCS™) website. NICCS is the one stop shop for cybersecurity careers and studies. There, you will find a wealth of information on the Workforce Framework. The site also connects you with information on:

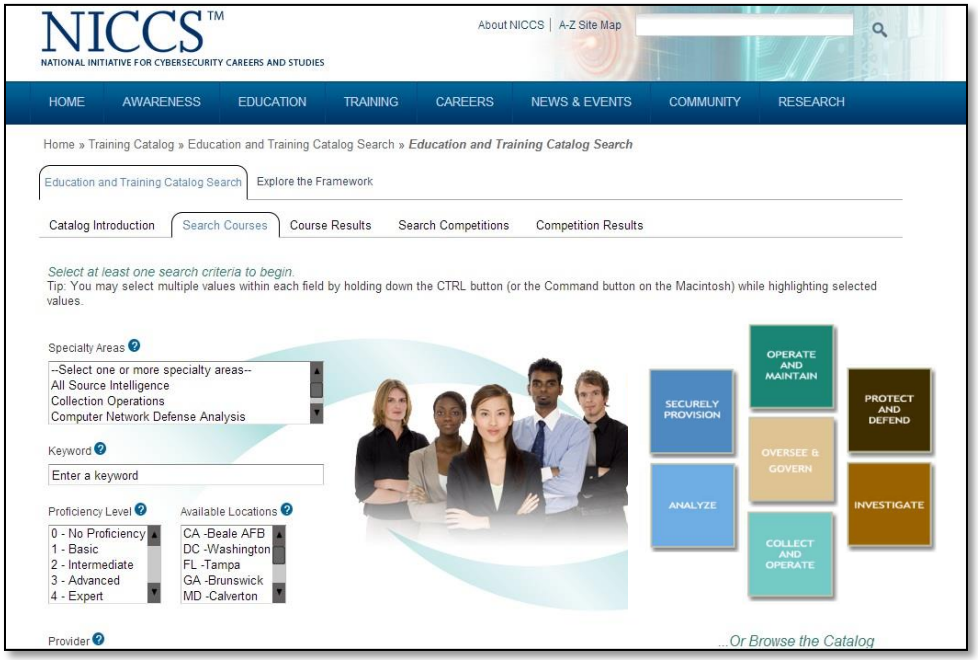
- Cybersecurity Awareness
- Professional Certifications and Courses
- Academic and Hands-on Learning Opportunities
- Workforce Development Strategies
- Federal Cybersecurity Training Events (FedCTE)
- Federal Virtual Training Environment (FedVTE)

Visit NICCS: www.niccs.us-cert.gov/

Searching the Training Catalog

You can search the Cybersecurity Education and Training Catalog by:

- Workforce Framework Specialty Area
- Course Title
- Course Proficiency Level
- Keyword
- Location
- Training Provider



Adding Courses to the Training Catalog

Information about how to add training courses to the Cybersecurity Education and Training Catalog is available by accessing the ***TRAINING*** tab.

On the Training landing page, click either "***Call for Providers***," or the "***Submit Training***" button to learn more.

Adding Courses to the Training Catalog - Four Step Process

The success of the Cybersecurity Education and Training Catalog depends on the completeness and accuracy of course information.

To add your courses to the Cybersecurity Education and Training Catalog:

1. **Apply –** Complete the NICCS Portal Provider Webform to establish a provider profile. Send the completed Provider Profile template to the NICCS Supervisory Office (NICCS SO) via email.
2. **Map –** Enter your training course information (either use the webform on NICCS for a single course, or download the Training Collection Template to enter multiple courses). Map your courses to the Workforce Framework's Specialty Areas.
3. **Submit –** Submit your training information to NICCS Supervisory Office (NICCS SO) via NICCS.
4. **Verify –** Verify your training information is posted properly.

Step 1: Apply to be an Approved Training Provider

The first step to adding your training courses to the Cybersecurity Education and Training Catalog is to become an approved NICCS Training Provider.

Every Training Provider is asked to provide information about their organization. This information is reviewed against a set of established vetting criteria. After the vetting process is completed and the Training Provider is approved, you will create your Provider Profile.

- Fill out the NICCS Portal Provider Webform.
- You will receive an email confirming receipt. If the NICCS SO has additional questions, a representative will contact you using the contact information provided.
- Once approved, you receive a unique **NICCS Provider ID** to use for future correspondence and training submissions.

Step 2: Map Training Courses to the Workforce Framework

Each course must be mapped to the Workforce Framework Specialty Area(s). Your **NICCS Provider ID** allows you to compile and prepare training information for inclusion in the Training Catalog. To map, select the Specialty Area proficiency level that best reflects the level of instruction for a given course. This information helps individuals in selecting the right level of training.

- Courses that teach content at Proficiency Level1 or higher must map to only one (1) Specialty Area.
- Courses that are Basic/Introductory, cover multiple Specialty Areas, and teach all content at Proficiency Level 1 may be mapped to up to three (3) Specialty Areas.

Level	Proficiency Level Description
0	This training is intended for someone with insufficient knowledge, skill, or ability level necessary for use in simple or routine work situations. Knowledge, skill, or ability level provided would be similar to the knowledge of a layperson. Considered "no proficiency" for purposes of accomplishing specialized, or technical, work.
1	This training is intended for individuals who need **basic knowledge, skills, or abilities** necessary for use and the application in simple work situations with specific instructions and/or guidance.
2	This training is intended for individuals who need **intermediate knowledge, skills, or abilities** for independent use and application in straightforward, routine work situations with limited need for direction.
3	This training is intended for individuals who need **advanced knowledge, skills, or abilities** for independent use and application in complex or novel work situations.
4	This training is intended for individuals who need **expert knowledge, skills, or abilities** for independent use and application in highly complex, difficult, or ambiguous work situations, or the trainee is an acknowledged authority, advisor, or key resource.

Step 3: Submit Courses to the Training Catalog

After you have mapped your course(s) to the Workforce Framework Specialty Area(s), you can submit your training information in two ways:

To upload a single course:

- Go to the NICCCS website to access the NICCS Course Webform.
- Complete the NICCS Course Webform with course information; submit the webform via NICCS.

OR

To upload multiple courses:

- Complete the **Training Catalog Data Collection Form** (excel template) provided in the email with your NICCS Provider ID.
- Email the file to NICCS SO.

You will receive a response from the NICCS SO after the course(s) are approved.

Step 4: Verify Data within the Training Catalog

Lastly, your training course information should be verified and updated on an ongoing basis.

- You will receive a notification when your training is initially uploaded to the Cybersecurity Education and Training Catalog .
- At that time, you can verify your training is described accurately and your provider contact information is correct.
- You must review your training course information on a regular basis and submit updated information as needed, especially if a course changes or is no longer offered.

Contact the NICCS SO if you need assistance posting or editing your training course information.

Contact Us

To learn more about the Workforce Framework and other Cybersecurity Education and Awareness (CE&A) Programs please contact:

Robin "Montana" Williams
Branch Chief, DHS Cybersecurity Education & Awareness
Phone: (703) 235-5169
Email: robin.williams@hq.dhs.gov

Kristina Dorville
Deputy Branch Chief, DHS Cybersecurity Education & Awareness
Phone: (703) 235-5281
Email: kristina.dorville@hq.dhs.gov